

Attachment A

FAX

Date 09/15/97

Number of pages including cover sheet 11

TO: Ken Allen
Townsend, Townsend & Crew

Phone 415 326 2400
Fax Phone 415 326 2422

FROM: Peter Marschall
SourceNet Corporation

Phone 702-332-3200
Fax Phone 702-332-3210

CC:

REMARKS: ☐ Urgent ☒ For your review ☐ Reply ASAP ☐ Please Comment

Attachment A

The On Demand Network
White Paper
DRAFT

CONFIDENTIAL

Attachment A

ODN - The On Demand Network

Digital Broadcast Television channels, thousands of true Video on Demand titles, Ultra High-Speed Internet Access, Video Conferencing, Local & Long Distance Voice Service - all delivered seamlessly from the same service provider - all delivered over a single physical transport medium to the end user.

This white paper will discuss a general background into the technology behind the On Demand Network, and it's current configuration and delivery mechanism. Issues of specific applications, content usage, advertising, billing and tracking systems will be discussed on a later paper.

BACKGROUND

The underlying theory of ODN:

- *Utilize current standards for the Internet communications Protocol (IP) for seamless delivery of all services.*
- *Utilize ATM network backbone architecture to ensure reliable delivery of service.*
- *Utilize cost effective last mile technology to deliver broadband service.*

On a Local Area Network (LAN), messages are sent between machines by supplying the six byte unique identifier (the "MAC" address). On top of these local or vendor specific network addresses, a unique number is assigned to every workstation, set-top box, or host. IP forwards each packet based on this destination address (the IP number). This IP number is a four byte value that, by convention, is expressed by converting each byte into a decimal number (0 to 255) and separating the bytes with a period. For example, the SourceNet server is 206.100.10.150. Thus, all information passed around the network is "packetized" and routed to it's destination via IP. The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world. Traditionally, TCP - is responsible for verifying the correct delivery of data from client to server, however TCP/IP is limited.

Connectionless networks, the type TCP/IP supports, do not commit network resources to particular conversations because all information travels across the network without using a specified route. Mechanisms for specifying the quality of service (QoS) required by TCP/IP applications are so primitive that they have never been implemented on any scale. TCP/IP does not provide applications with predictable performance, or allow users to control how network costs are traded against performance for any application or set of applications.

This situation was tolerable in the early days of TCP/IP, when business commitments to the protocol were light. It is not tolerable in a world where most traffic is carried via TCP/IP. Business invests in networks to support crucial applications. Crucial applications need controlled response times. Thus IP will be used to address the network and pass virtual routing information along to an ATM route manager which will setup a "switched virtual circuit" to the end host. Data will then be cell-relayed along those routes ensuring delivery and specifying QoS.

It is important to understand the end-to-end network topology of the ODN delivery service at this time (Please refer to Appendix B). Every device that provides ODN content services (Mpeg Encoders, Video Servers, Internet routers, etc.) will be connected to the ATM backbone directly. Some services and content will be delivered from a more centralized location-Internet gateway access and Broadcast digital television. Other services and content will be delivered farther out in the network-Video on Demand service and voice access to the Public Switched Telephone Network (PSTN). At the remote service node, we connect a Digital Subscriber Line (DSL) transport system to the ATM network which provides high-speed point-to-point connectivity between the end users premise, our ATM network, and the PSTN. DSL utilizes standard twisted pair copper

Attachment A

connectivity-digitally modulated or separated into channels for data and voice delivery. Asymmetrical Digital Subscriber Line or ADSL provides bi-directional data transport at asymmetrical data rates. Typically an end user will receive 6-Mb/sec downstream and roughly 10% of that rate upstream. A separate channel carries lifeline POTS (Plain Old Telephone Service) to the users premise. Once in the home, the POTS is split into the existing phone network in the home (it is important to note here that voice service is completely passive and will still function in the event of power outage). The data channels are then directed via a separate data network (ethernet over CAT 5 wire) to each host (computer with ethernet interface, digital set-top box, etc.).

CONTENT DEVICES AND DELIVERY SERVICES

Broadcast Digital Television. In the current trial, the SourceNet Head-end consists of a satellite receiving system that routes 32 channels of analog Broadcast television to a bank of Mpeg encoders (please see diagram Appendix C). These encoders turn each channel into a digital signal that is "packetized," addressed with a unique IP number, and dropped onto the network.

ODN utilizes IP multicast to deliver Digital Broadcast Television Channels to the end host. Multicasting (directing the same information packets to multiple destinations at the same time) is much more efficient than unicasting (sending a separate copy to each individual destination). The benefits of IP Multicasting are: 1) the sender only has to send out one copy of the information packet instead of many, 2) the information is delivered in a more timely, synchronized fashion because all destinations receive the same source packet, 3) multicasting can be used to send information to destinations whose individual addresses are unknown (similar to a broadcast), and 4) It reduces the overall number of packets on the network (that is, one multicast packet sent instead of many unicast packets).

There is a fixed amount of bandwidth that exists between the SourceNet head-end and each remote node. Because of the nature of multicast all of the channels can be delivered to a virtually unlimited number of remote users-and the amount of bandwidth utilization along the path to the remote nodes remains fixed. Packet replication occurs at the closest point to the end user-down their last mile delivery circuit.

Multicast address are like IP addresses used for single hosts, and is written in the same way: A.B.C.D. Multicast addresses will never clash with host addresses because a portion of the IP address space is specifically reserved for multicast. This reserved range consists of addresses from 224.0.0.0 to 239.255.255.255. However, the multicast addresses from 224.0.0.0 to 224.0.0.255 are reserved for multicast routing information; Application programs should use multicast addresses outside this range.

Sending a multicast datagram is easy. The Mpeg encoders simply specify a multicast address as the destination. To receive multicast packets, an application must first request that the host join a particular multicast group.

In addition to the host part of an IP multicast address, there is also a port number, as in TCP or UDP sockets. This port number information is used by the kernel to decide which port on the local machine to route packets to.

Unfortunately networks without some type of multicast control treat a multicast as a broadcast. This means that all hosts that reside in a destination network must process all multicasts sent to that network. In an environment rich in multicast types of applications, this could require performance robbing CPU cycles from all hosts on the network. Internet Group Management Protocol (IGMP) was developed to address this problem (Please see Appendix E for a complete description of IGMP).

Customer premise host issues as they relate to IGMP will be discussed further on.

Internet Access. Internet access for all customers of the ODN system will come from the SourceNet internet gateway in downtown Reno. Each will have a dedicated "pipe" to

Attachment A

the Internet, however, the actual virtual circuit from their host to the gateway router will be setup dynamically as it is needed.

Video on Demand. Unlike digital televisions point to multi-point (multi-cast) distribution method, Video on Demand (VoD) is a point to point (unicast) distribution method. Since it is more difficult to determine how many users will use the VoD service concurrently, the bandwidth utilization is unpredictable. Therefore, a distributed VoD topology is necessary. The concept is to place Video on Demand servers as close to the end users as possible, where increasing network capacity is the most cost effective at the remote nodes.

Content is obtained to a particular host (a set-top box connected to a television for example) through the use of Web servers which provide the menus and interfaces necessary to order a title. The Web server then communicates with the Video servers that "stream" video content to the correct destination host IP address. In this case, packets received by the set-top box from the video server are processed, the Mpeg video is extracted and decoded to the television set.

Today's video servers provide many advanced features to the end user. The latest implementation allows for full VCR-like functionality over a film. Users have the ability to pause, fast forward, and rewind a film in progress thus providing a distinct interactive advantage over traditional Near Video on Demand or Pay-per-view services.

Voice Service. Voice Service will be provided seamlessly through the Digital Subscriber Line system. POTS splitters allow connectivity to the Public Switched Telephone Network to be seamlessly modulated onto a DSL circuit, and then distributed to and throughout the customer's home telephone plant. The use of the phone does not affect, nor is affected by the simultaneous use of other digital services (access to the Internet, watching a movie, etc.)

CUSTOMER PREMISE EQUIPMENT

Once the in-home network has been installed, any IP addressable device can be attached via 10bT or ATM interface to have access to the services. These devices consist mainly of computers and digital set-top boxes. Recent trends in the purchase of digital set-top boxes to browse the Internet indicate that consumers are highly interested in utilizing the less intimidating interface of a remote control and their TV to view World Wide Web content. Many consumers don't have the knowledge or interest necessary to install and configure their personal computer to take advantage of the enhanced ODN system. Therefore, we will provide a set-top box capable of receiving all types of content from our system to the TV.

The set-top box will be connected via network interface and will have it's own unique IP number. It's main interface will consist of a Web browser. The menus presented will allow users to access the Internet directly, order videos on demand, and view network and cable television.

Today's set-top boxes provide users with access to most of the content that ODN will provide with the exception of the reception of digital broadcast television. This requires the implementation of IGMP (discussed earlier, please see Appendix E). SourceNet Corporation will develop this component for the set-top boxes that integrate into our system

CONCLUSION

The first of it's kind-ODN will seamlessly deliver traditional and enhanced content from a single provider. Internet technology has introduced a more interactive approach of content delivery to a global market. By adding digital broadcast content and true Video on Demand service to this type of delivery mechanism, enhancing it's delivery system, ensuring quality of service, and including traditional voice service SourceNet Corporation has developed a unique product for the households of the 21st century.

Attachment A

APPENDIX A

**Protocol Layering
The OSI Reference Model**

The seven layer reference model for open systems interconnection, developed by members of the International Standards Organization (ISO) and documented in ISO 7498, that provides a common basis for the coordination of standards for the purpose of systems interconnection. Each layer has defined function, or set of functions. An interface defined between layers to enforce a structured design paradigm.

The First three layers are thus defined:

**Layer 1 - Physical Layer
Functions of the Physical Layer:**

The physical layer is responsible for the actual transmission of a bit stream across a physical circuit. It allows signals, such as electrical signals, optical signals, or radio signals, to be exchanged among communicating machines. The physical layer typically consists of hardware permanently installed in the communicating devices. The physical layer also addresses the cables, connectors, modems, and other devices used to permit machines to physically communicate.

Physical layer mechanisms in each of the communicating machines typically control the generation and detection of signals that are interpreted as 0 bits and 1 bits. The physical layer does not assign any significance to the bits. For instance, it is not concerned with how many bits make up each unit of data, nor is it concerned with the meaning of the data being transmitted. In the physical layer, the sender simply transmits a signal and the receiver detects it.

**Layer 2: Data Link Layer
Functions of the Data Link Layer:**

The data link layer is responsible for providing data transmission over a single connection from one system to another. Control mechanisms in the data link layer handle the transmission of data units, often called frames, over a physical circuit. Functions operating in the data link layer allow data to be transmitted, in a relatively error-free fashion, over a sometimes error-prone circuit.

This layer is concerned with how bits are grouped into frames and performs synchronization functions with respect to failures occurring in the physical layer. The data link layer implements error-detection mechanisms that identify transmission errors. With some types of data links, the data link layer may also perform procedures for flow control, frame sequencing, and recovery from transmission errors.

**Layer 3: Network Layer
Functions of the Network Layer:**

The network layer is concerned with making routing decisions and relaying data from one device to another through the network. The OSI model classifies each system in the network as one of two types: end-systems act as the source or the final destination of data, and intermediate systems perform routing and relaying functions. The facilities

Attachment A

provided by the network layer supply a service that higher layers employ for moving data units, often called packets, from one end system to another, where the packets may flow through any number of intermediate systems.

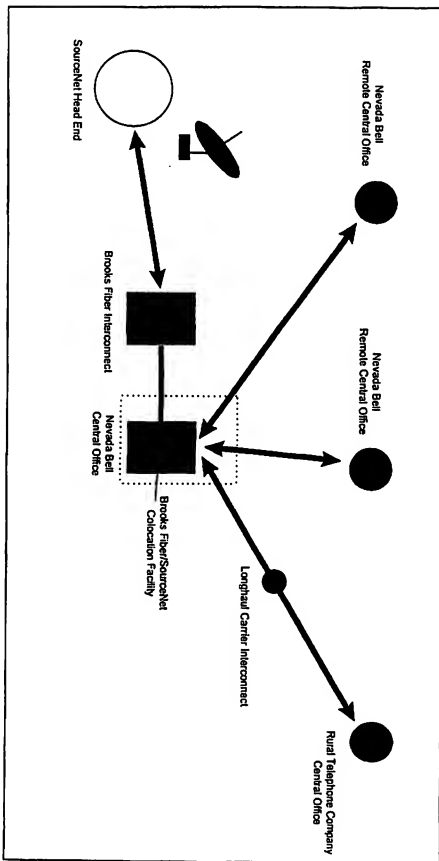
End systems generally implement all seven layers of the OSI model, allowing application programs to exchange information with each other. It is possible for intermediate systems performing only routing and relaying functions to implement only the bottom three layers of the OSI model.

In a complex network, the path between any two systems may at one instant be via a number of data links. The application programs running in two end systems that wish to communicate should not need to be concerned with the route packets take nor with how many data links they must cross. Network layer functions operating in end systems and in intermediate systems together handle these routing and relaying functions.

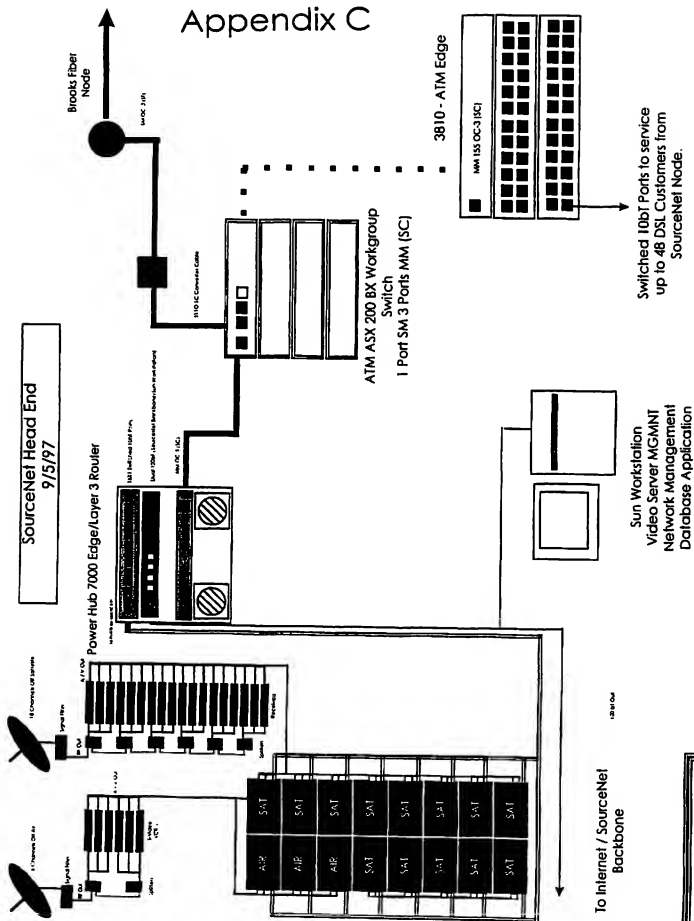
Whereas the data link layer provides for the transmission of frames between adjacent systems across a single data link, the network layer provides for the much more complex task of transmitting packets between any two end systems in the network, regardless of how many data links may need to be traversed.

Attachment A

Appendix B

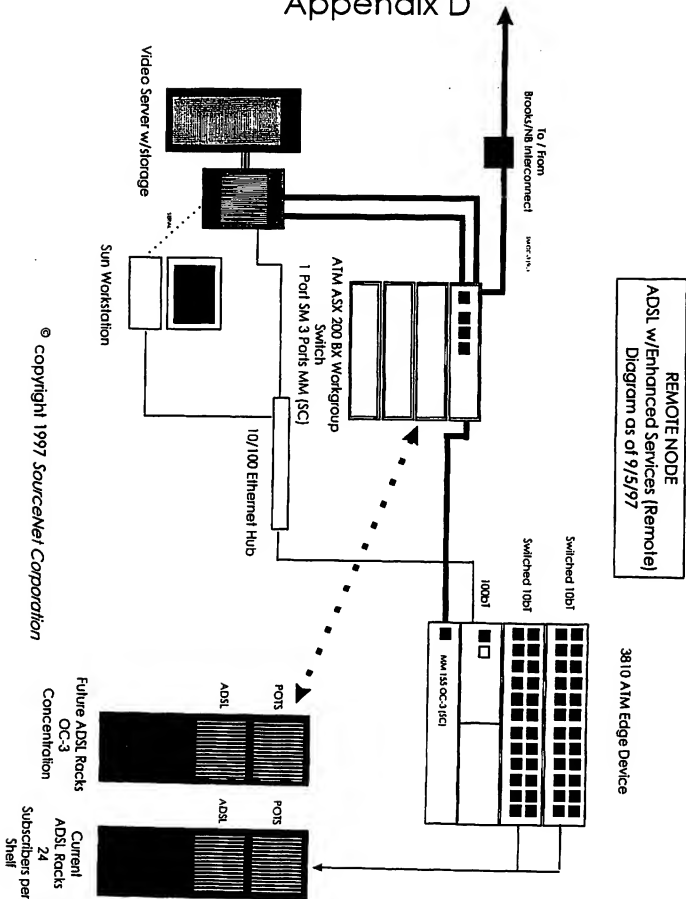


Appendix C



Attachment A

Appendix D



Attachment A

APPENDIX E

Internet Group Management Protocol (IGMP), an internal protocol of the Internet Protocol (IP) suite, provides a means to automatically control and limit the flow of multicast traffic through the network. Applications that implement IGMP, on networks that support IGMP, effectively eliminate multicast traffic on segments that are not destined to receive this traffic.

IGMP manages multicast traffic throughout networks with the use of special multicast queriers and hosts that support IGMP. (A "querier" is a network device that sends queries. It is typically a router but can be another type of device that is designed to behave as a querier, such as switches that support this feature). Each set of queriers and hosts that send and/or receive multicast data streams from the same set of sources is called a multicast group. IGMP identifies members of the multicast group per "subnet" and provides mechanisms (messages) by which queriers and hosts can join and leave multicast groups.

The queriers and hosts use three specific message structures, "query", "report", and "leave group", to communicate to each other about the multicast traffic. Query messages are used by queriers to discover which network devices are members of a given multicast group. Report messages are sent by hosts in response to queries to inform the querier of a host's membership. The host may also use the report message to join a new group. Leave group messages are sent when the host wishes to leave the multicast group.

Information courtesy of Hewlett Packard. On the Internet:
<http://hpcc920.external.hp.com/md/technol/whtpaper/switch/igmp/igmp.htm>